S5120-EI系列交换机下连PC客户端认证下线后MAC地址没有被交换机自动删除的解决方法

岳斌 2010-10-21 发表

S5120-EI系列交换机下连PC客户端认证下线后MAC地址没有被交换机自动删除的解决方法

一、 组网：

PC客户端直连AVAYA IP电话，该电话又直连在S5120-EI系列交换机上，交换机与Radius服务器路由可达。该电话进行EAP-MD5认证，PC客户端通过EAP-TLS认证。

二、 问题描述：

在S5120-EI系列交换机上主要配置如下。

```
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2602 untagged
 port hybrid pvid vlan 2602
 undo voice vlan mode auto
 voice vlan 2602 enable
 mac-vlan enable
bpdu-drop any
stp edged-port enable
 lldp compliance admin-status cdp txrx
 port-security port-mode userlogin-secure-ext
 dot1x guest-vlan 10
 dot1x auth-fail vlan 10
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
```

正常情况下，PC客户端与AVAYA IP电话通过认证后，在交换机上可以找到PC客户端与IP电话在各自VLAN中的MAC地址，当通过拔掉PC与IP电话间网线的方式让PC下线后，仍然可以在交换机上找到PC的MAC地址。

三、 过程分析：

AVAYA电话下连PC下线后（即将网线拔掉后），AVAYA电话会发送标准的EAP logoff报文给交换机。如果交换机端口上配置了bpdu-drop any命令，交换机会将该报文丢弃，但是为何认证前的EAP报文没有被交换机丢掉呢？原因如下。

认证通过前交换机收到的认证报文携带的是未知源MAC，直接被上送到CPU处理，其优先级高于bpdu-drop any命令；但是认证通过以后，交换机已经记录下客户端的源MAC地址（现在应经变为已知源MAC了），那么对于携带已知源MAC的报文，交换机处理机制就变化了，即通过匹配ACL的方式上送CPU处理，此时由于bpdu-drop any的优先级高于已知源MAC的报文，所以EAP logoff的报文就丢掉了。

四、 解决方法：

将端口下bpdu-drop any的命令去掉，如果想实现同样的功能，可在端口下使用stp disable命令。